计算机网络安全技术

李巍
liw@buaa.edu.cn

北航计算机学院
2018年春季

目 标

- 理解计算机网络安全的基本概念、原理和知识结构
- 掌握计算机网络安全技术的基本原理、方法和工具
- 掌握主流的网络攻防基础方法和技术
- 了解Internet的安全性，增强安全意识

课程安排

- 本课程所需基础知识
  - 计算机网络、密码学、操作系统、程序设计（C，Java，Python）等
- 授课方法
  - 课堂讲解+自学+课后作业+课程设计project
- 课件、课程资料、作业
  - 课程中心网站 course.buaa.edu.cn
- 考核方式
  - 考勤：5%
  - 作业：45%
    - 小作业（2次）：共20%
    - 课程设计大作业1次：25%
  - 期末考试：50%
    - 2小时，开卷

参考书目

- William Stallings，网络安全基础-应用与标准（第5版），清华大学出版社，2014年5月
- William Stallings，Lawrie Brown，计算机安全原理与实践（第三版），机械工业出版社，2016年3月
- 斯坦普（Mark Stamp）著；张戈 译，信息安全原理与实践（第2版）[Information Security: Principles and Practice, 2nd Edition]，清华大学出版社，2013年5月

主要内容及课时安排

- 概述（2）
- 密码学基础（4）
  - 基本概念和方法；对称密码体系；公钥密码体系
- 身份认证与密钥管理技术（2）
- 访问控制技术（2）
- 网络安全基础设施（12）
  - 网络层相关协议；传输层相关协议
  - 应用层 相关协议（Internet）
  - 防火墙；入侵检测IDS；IPS
- 系统安全（6）
  - Web安全；匿名通信；安全管理
- 课堂讨论（4）

与计算机网络相关的基础知识

- 网络体系结构
  - ISO/OSI 参考模型
  - TCP/IP 协议栈
- 物理层和数据链路层
  - 全双工 vs. 半双工
  - CRC校验（Cyclic Redundancy Check）
  - 以太网 Ethernet
  - IEEE 802 MAC 地址
  - 桥接Bridging 和路由Routing
  - 无线局域网 IEEE 802.11 LAN

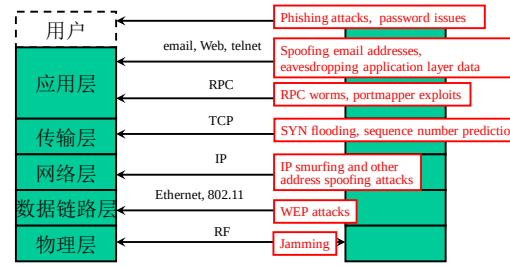
与计算机网络相关的基础知识（续）

◆网络层
- ❖IP 地址和子网 Subnets
- ❖私有地址 Private Addresses
- ❖ARP协议和ICMP协议
- ❖ IPV6 地址addresses
- ❖ 路由协议（RIP, OSPF, BGP）

◆传输层
- ❖TCP 协议
- ❖UDP协议
- ❖TCP 建立连接过程

◆应用层
- ❖web和HTTP协议
- ❖电子邮件
- ❖DNS

网络体系结构 vs. 网络安全



网络安全

◆Network Security → Cyber Security
网络安全　　网络空间安全

◆网络空间（Cyberspace）
- ❖1991年9月号《科学美国人》出版《通信、计算机和网络》专刊，第一次出现“网络空间Cyberspace”
- ❖是通过全球互联网和计算系统进行通信、控制和信息共享的动态（不断变化）虚拟空间*
- ❖在信息时代是社会有机运行的神经指挥系统，目前已经成为与陆、海、空、太空之后的第五空间。

*《积极构建网络空间安全创新人才培养体系》，http://www.cac.gov.cn/中共中央网络安全和信息化领导小组办公室

网络空间组成

◆由独立且互相依存的信息基础设施和网络组成，包括互联网、电信网、计算机系统、嵌入式处理器和控制器系统
- ❖网络互联而成的各种计算系统（包括各种智能终端）
- ❖连接端系统的网络
- ❖连接网络的互联网和受控系统
  - ➢硬件、软件乃至产生、处理、传输、存储的各种数据或信息

◆特点
- ❖没有明确的、固定的边界
- ❖没有集中的控制权威。

网络空间安全

◆网络空间安全（Cyberspace Security或简称Cyber Security）：研究网络空间中的安全威胁和防护问题
- ❖在有对手（adversary）的对抗环境下，研究信息在产生、传输、存储、处理的各个环节中所面临的威胁和防御措施、以及网络和系统本身的威胁和防护机制。
  - ➢信息的保密性、完整性和可用性
  - ➢网络空间基础设施的 安全和可信

信息安全 vs. 网络安全 vs. 网络空间安全

◆信息安全、网络安全、网络空间安全
- ❖核心是信息安全问题，只是出发点和侧重点有所差别
- ❖信息安全
  - ➢侧重于线下和线上的信息安全
- ❖网络安全
  - ➢侧重于线上安全和网络社会安全
- ❖网络空间安全
  - ➢侧重点是与陆、海、空、太空并列的空间概念

网络安全的重要性

- 云计算，物联网的普及，对信息传输、存储、共享的依赖，增加数字世界的风险
- 目前研究网络安全已经不只为了信息和数据的安全性
- 网络安全已经渗透到国家的政治、经济、社会稳定、军事等领域

安全事件- WannaCry勒索软件

- 2017年5月12日，WannaCry勒索软件席卷全球，此病毒共使100多个国家的数十万用户的计算机遭到攻击，其中包括医疗、教育等公共事业单位和一些大公司。
  - 这款蠕虫病毒对计算机内的文档、图片、程序等实施高强度的加密锁定，并向用户索取以比特币支付的赎金。
- 攻击者利用NSA(美国国家安全局)设计的Windows系统黑客工具“永恒之蓝Eternal Blue”。
  - 该病毒主要是利用Windows的445端口传播，该端口在Windows主要是提供局域网中文件或打印机共享服务。而此前部分运营商对个人用户封掉了445端口。
- 应对
  - 操作系统补丁升级：3月14微软已经发布补丁，由于很多受害者没有及时安装补丁，导致被病毒攻击。
  - 防火墙关闭相关端口

安全事件- Mirai僵尸网络

- 物联网Mirai僵尸网络攻击
  - 2016年10月21日，美国多个城市出现互联网瘫痪情况，包括Twitter、Shopify、Reddit等在内的大量互联网知名网站数小时无法正常访问。
  - 美国域名服务提供商Dyn公司遭到大规模的“拒绝访问服务（DDoS）”攻击。
- 后据调查，这是Mirai僵尸网络发动的攻击。Mirai僵尸网络中包含了大量可联网设备
  - 例如监控摄像头、路由器以及智能电视等等。
  - 有大约60万台的物联网设备参与

安全事件-心脏出血Heartbleed漏洞

- 开源软件包OpenSSL：提供主要的密码算法、常用的密钥和证书封装管理功能以及SSL协议
- 2014年4月爆出了OpenSSL的Heartbleed漏洞，该漏洞是近年来影响范围最广的高危漏洞，涉及各大网银、门户网站等。
  - 该漏洞可被用于窃取服务器敏感信息，实时抓取用户的账号密码
- OpenSSL又被曝出存在“水牢DROWN漏洞”（2016年3月）
  - 这一漏洞允许“黑客”攻击网站，并读取密码、信用卡账号、商业机密和金融数据等加密信息。
  - 由于全球2/3的网站服务器都是采用OpenSSL协议加密，为全球网站带来巨大安全挑战。
  - 这次安全漏洞涉及了全球400万家网站和服务器，其中，我国有十万余家网站受到影响。

安全事件-其他

- 中国互联网DNS劫持
  - 2014年1月21日下午3点10分左右，国内通用顶级域的根服务器忽然出现异常，导致众多知名网站出现DNS解析故障，用户无法正常访问。虽然国内访问根服务器很快恢复，但由于DNS缓存问题，部分地区用户“断网”现象仍持续了数个小时，至少有2/3的国内网站受到影响。
- Shellshock破壳漏洞
  - 2014年9月25日，US-CERT公布了一个严重的Bash安全漏洞(CVE-2014 -6271)。由于GNU Bash更广泛的存在，导致其所威胁到的不仅仅是服务器系统，也包括了网络设备、网络交换设备、防火墙等网络安全设备，也包括摄像头、IP电话等很多采用Linux定制的系统。
- IE的0Day漏洞，……


数据泄露

数据泄漏

- 雅虎共超15亿用户信息遭窃
- 2.7亿Gmail、雅虎和Hotmail账号遭泄露
- “希拉里邮件门”事件
- 4.27亿MySpace数据泄漏
- 索尼影业公司被黑客攻击
- iCloud数据泄露
- eBay数据泄露事件
- ……

恶意软件Malware的类型

- 病毒Viruses
  - Code that attaches itself to programs, disks, or memory to propagate itself
- 蠕虫Worms
  - Installs copies of itself on other machines on a network, e.g., by finding user names and passwords
- 木马 Trojan horses
  - Pretend to be a utility. Convince users to install on PC
- Rootkit
  - 监控程序，Gets “root” (admin) privilege
- Spyware
- Key Loggers，Hoax，Trap Door，Logic Bomb，Zombie，…

计算机病毒（Computer Virus）

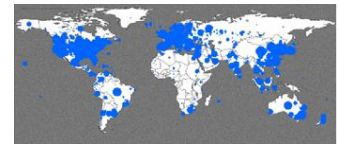
- 《中华人民共和国计算机信息系统安全保护条例》中的相关定义
  - “指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码”。
- 病毒必须满足两个条件：
  - 能自行执行。它通常将自己的代码置于另一个程序的执行路径中。
  - 能自我复制。例如，它可能用受病毒感染的文件副本替换其他可执行文件。
- 病毒既可以感染桌面计算机也可以感染网络服务器。
- 病毒往往还具有很强的感染性，一定的潜伏性，特定的触发性和很大的破坏性等。

蠕虫Worm

- 通过网络连接进行传播的恶意程序
  - 它具有病毒的一些共性，如传播性、隐蔽性、破坏性等等，同时具有自己的一些特征，如不利用文件寄生（有的只存在于内存中），对网络造成拒绝服务，以及和黑客技术相结合。
  - 典型的蠕虫病毒有尼姆达、震荡波、熊猫烧香等。
- 历史
  - 1998年11月， Morris 蠕虫通过邮件服务器进行传播
  - 2001年，“Code Red”蠕虫 攻击了Internet上约 360,000台PC机。感染数量每37分钟翻一番。
  - 2004年，“Witty” 蠕虫感染特定网络安全产品：ISS “Black Ice” and “Real Secure.” 45分钟内感染了大量系统.

蠕虫Worm

- 例：2003年1月25日，SQL Slammer（又名：Sapphire爆发，它是曾经出现过的传播速度最快的蠕虫，每隔8.5秒的时间它所感染的主机的数目就要翻一番，在10分钟的时间内它就感染了近90%的脆弱性主机。该蠕虫利用的是SQL服务器或MSDE 2000中包含的缓冲区溢出漏洞。



Spread of Sapphire virus, after 38 minutes.

木马（Trojan Horse）

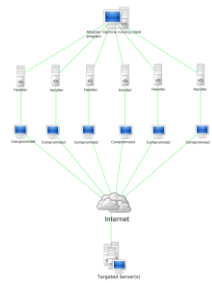
- 木马正是指那些表面上是有用的软件、实际目的却是危害计算机安全并导致严重破坏的计算机程序。
  - 是一种基于远程控制的黑客工具，具有欺骗性、隐蔽性和非授权性的特点。
  - 隐蔽性：是指木马的设计者为了防止木马被发现，会采用多种手段隐藏木马，这样服务端即使发现感染了木马，也难以确定其具体位置；
  - 非授权性：是指一旦控制端与服务端连接后，控制端将窃取到服务端的很多操作权限，如修改文件，修改注册表，控制鼠标，键盘，窃取信息等等。

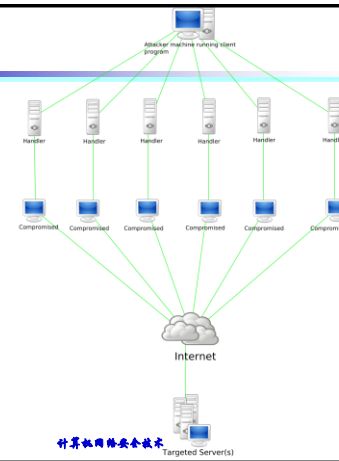
Rootkit

- Rootkit是一种特殊的恶意软件
- 是在安装目标上隐藏自身及指定的文件、进程和网络链接等信息，比较多见到的是Rootkit一般都和木马、后门等其他恶意程序结合使用。
- Rootkit通过加载特殊的驱动，修改系统内核，进而达到隐藏信息的目的。

僵尸网络Botnet

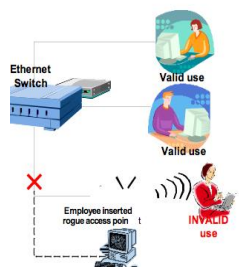
- 演化：二十世纪末期，蠕虫演化为僵尸网络 "Bot" (for Robot)
  - 2008年11月，“Conficker” 感染了大约1千万台计算机；每天发送约 10亿封 垃圾邮件和钓鱼邮件
- 作用
  - 发送垃圾邮件（Spam）和钓鱼邮件（ Phishing ）
  - 控制其他计算机
  - 发动攻击：如分布式拒绝服务攻击(DDOS)





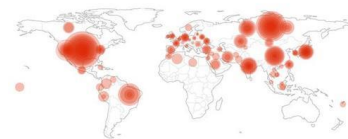
无线网的安全问题

- 无线网络的普及
  - 2010年，无线网络广泛部署
- WiFi的安全问题
  - 加密方法的问题: WEP和WPA被破解
  - 非法接入点(Rogue AP)

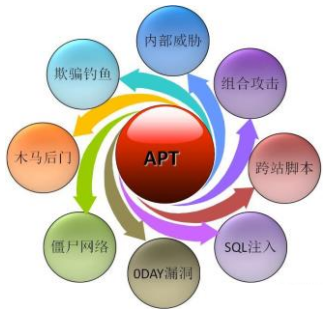


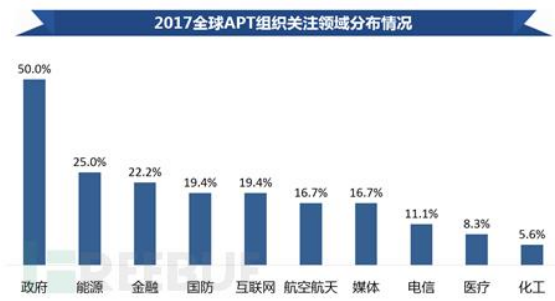
APT

- APT(Advanced Persistent Threat，高级持续性威胁)
  - 2014年被曝光的APT事件攻击了近百个国家，其中遭受攻击最多的也正是美国、俄罗斯、中国、日本等全球国家。主要被攻击的行业为能源、金融、医疗保健、媒体和电信、公共管理、安全与防务、运输和交通等行业。
- Spear Phishing：the Most Common Attack
  - 90%以上的APT目标攻击采用鱼叉式网络钓鱼攻击手法



APT





2017 中国高级持续性威胁（APT）研究报告

http://www.freebuf.com/articles/network/163435.html

网络安全的挑战

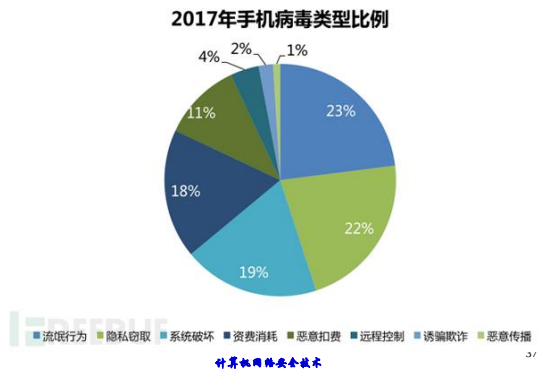
- 复杂性
  - 多种安全机制，部署方法，信任问题
- 考虑潜在攻击和多种威胁
- 包括算法和一些机密信息
- 攻防的较量：人
- 成本
  - 定期监控；事后考虑
- 影响系统的有效性和易操作性

目前网络安全形势

- 维护网络安全首次列入我国政府工作报告
  - 2014年2月27日，中央网络安全和信息化领导小组宣告成立
  - 研究制定网络安全和信息化发展战略，不断增强国家安全保障能力
  - 信息安全问题上升到国家战略层面
- 各国加速网络安全战略部署
  - 美国从90年代后期开始注重关键基础设施来自网络空间的威胁，并先后制定出成熟的国家网络空间安全战略，2014年2月，美国总统奥巴马宣布启动美国《网络安全框架》
  - 欧洲各国合作保障升级，加强网络安全立法，以应对日益严峻的网络攻击。
  - 日本尤其注重保障个人信息安全，大力发展网络作战能力。

2017中国网络安全报告

http://www.freebuf.com/articles/paper/161600.html



网络安全威胁来自哪里

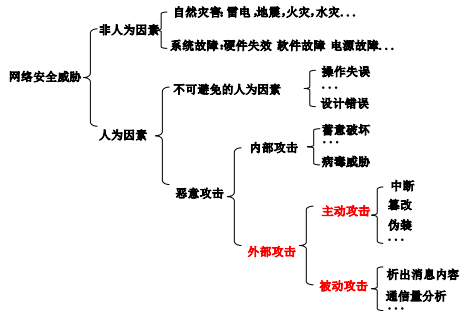
- 内因
  - 人们的认识能力和实践能力的局限性
  - 系统软件规模的庞大
  - 系统自身的脆弱性
    - 网络的开放性
    - 黑客（Hacker）及病毒等恶意程序的攻击
    - 系统平台系统软件的自身缺陷
    - TCP/IP分层体系结构的脆弱性
    - 操作系统及数据库的脆弱性
  - 网络误用/滥用
  - 没有良好的管理机制

安全威胁来自哪里

- 外因

国家安全威胁	信息战士	减小决策空间、战略优势，制造混乱，进行目标破坏
	情报机构	搜集政治、军事，经济信息
共同威胁	恐怖分子	破坏公共秩序，制造混乱，发动政变
	工业间谍	掠夺竞争优势，恐吓
	犯罪团伙	施行报复，实现经济目的，破坏制度
局部威胁	社会型黑客	攫取金钱，恐吓，挑战，获取声望
	娱乐型黑客	以吓人为乐，喜欢挑战

网络安全威胁分类



第一章 概述

信息安全

- 信息安全保障的需求
  - 物理方法
  - 管理方法
- 引入计算机和互联网络
  - 计算机安全
  - 网络安全
- 信息安全是一门交叉学科。
  - 广义上，信息安全涉及多方面的理论和应用知识，除了数学、通信、计算机等自然科学外，还涉及法律、心理学等社会科学
  - 狭义上，也就是通常说的信息安全，只是从自然科学的角度介绍信息安全的研究内容

计算机安全

- 美国国家标准与技术研究院（NIST）计算机安全手册的定义
  - 对某个自动化信息系统的保护措施，其目的在于实现信息系统资源的*完整性、可用性和机密性*（包括硬件、软件、固件、数据/信息、电信）

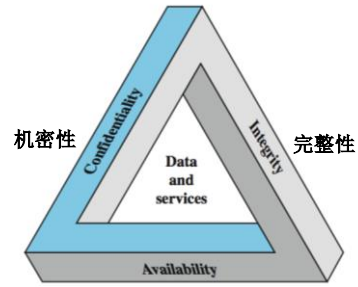
“the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications”

网络安全（Network Security）

- 涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科
- 分布式网络环境中，对信息载体（处理载体、存储载体、传输载体）和信息处理、传输和存储、访问提供安全保护，以防止数据、信息内容、处理能力等被拒绝服务或被非授权使用和篡改

核心概念：CIA三元组

Confidentiality, Integrity and Availability



核心概念：CIA三元组

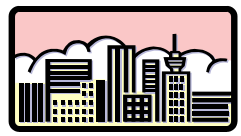
- 机密性Confidentiality
  - 机密性是指保证信息不能被非授权访问，即使非授权用户得到信息也无法知晓信息内容，因而不能使用
    - 数据机密性
    - 隐私性
- 完整性Integrity
  - 完整性是指维护信息的一致性，即信息在生成、传输、存储和使用过程中不应发生人为或非人为的非授权篡改。
    - 数据完整性
    - 系统完整性
- 可用性Availability
  - 可用性是指保障信息资源随时可提供服务的能力特性，即授权用户根据需要可以随时访问所需信息

计算机和网络安全的挑战

1. 安全机制的复杂性
2. 安全机制要考虑潜在攻击和各种威胁
3. 安全机制的部署方法
4. 可信的通信协议，保护机密信息的方法
5. 攻防双方（人）的较量
6. 直到灾难发生才能察觉
7. 需要定期监控
8. 通常是事后考虑
9. 影响系统的有效性和易操作性

OSI Security Architecture

- OSI安全体系结构
  - ITU-T X.800 “Security Architecture for OSI”
- 定义了系统级方法
  - defines a systematic way of defining and providing security requirements
- 国际标准
  - 提供概念模型

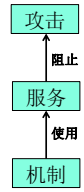


OSI安全体系结构

- 信息安全的三个方面
  - 安全攻击 security attack
  - 安全机制 security mechanism
  - 安全服务 security service

基本概念

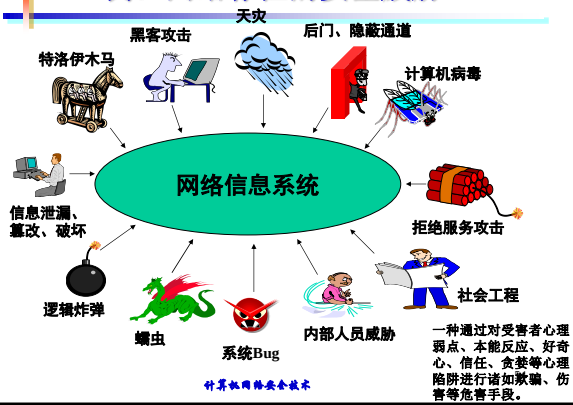
- 攻击attack
  - 安全攻击：任何破坏信息安全的行为。 (e.g., stealing information).
- 机制mechanism
  - 安全机制：用来检测detect、阻止prevent安全攻击，或从攻击中恢复recover的机制。(e.g., encryption)
- 服务service
  - 安全服务：增强数据处理系统和信息传输的安全性的服务。安全服务可以利用一个或多个安全机制。 (e.g., SSL for Web browsers and servers).



威胁 vs. 攻击

- 两个概念
  - 威胁 *threat* – a potential for violation of security
  - 攻击 *attack* – an assault on system security, a deliberate attempt to evade security services

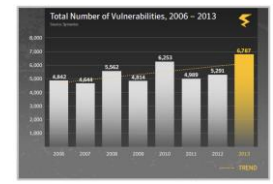
例：网络存在的安全威胁



一种通过对受害者心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱进行诸如欺骗、伤害等危害手段。

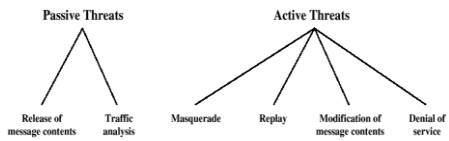
例：网络威胁统计

- 国外
  - Computer Emergency Response Team
    - www.us-cert.gov
  - www.sans.org
- 国内
  - 国家互联网应急中心 http://www.cert.org.cn/
  - 国家信息安全漏洞共享平台（China National Vulnerability Database，简称CNVD） http://www.cnvd.org.cn/
- 网络安全厂商



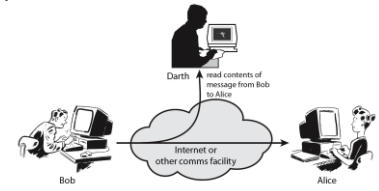
安全威胁/攻击

- 安全威胁/攻击(Security Threats/Attack）
  - 被动攻击Passive Threats
  - 主动攻击Active Threats



网络攻击方式:被动攻击

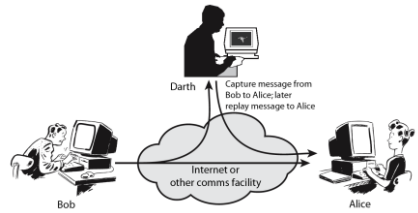
- 被动攻击
  - 消息内容泄露：窃听或者偷窥
  - 流量分析攻击



应对被动攻击：防范（如加密）

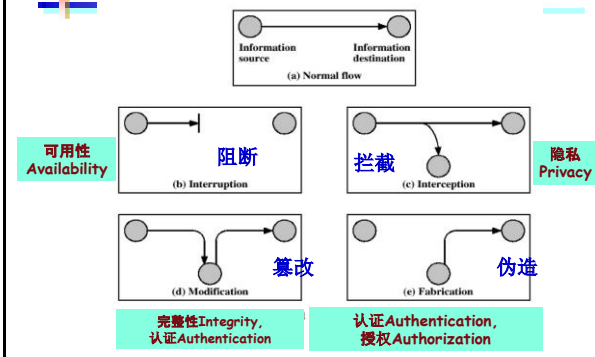
网络攻击方式：主动攻击

- 主动攻击
  - 指攻击者对某个连接中的数据进行各种处理(阻断、拦截、伪造、重放、篡改、拒绝服务等)



应对主动攻击：检测和恢复

主动攻击的几种类型



安全服务

- X.800的定义
  - 由通信开放系统的协议层提供的，并能确保系统或数据传输足够安全的服务
  - 5类14种特定服务（表1.2）
- RFC2828
  - 由系统提供的对系统资源进行特定保护的处理或通信服务。

安全服务实现安全策略

安全机制实现安全服务

安全服务（X.800）

- 五类可选的安全服务
  - 认证/鉴别Authentication：鉴别用于保证通信的真实性
  - 访问控制Access Control：防止对网络资源的非授权访问
  - 数据机密性Data Confidentiality：保护数据以防止被动攻击
  - 数据完整性Data Integrity：保证所接收的消息未经复制、篡改、插入、重排或重放，既用于对付主动攻击
  - 不可否认Non-Repudiation：防止通信双方中的某一方抵赖所传输的消息

安全服务（X.800）

- 认证 Authentication
  - 用户登录认证
  - 消息认证
- 访问控制access control 和授权 Authorization
  - 防止资源被误用
- 机密性和隐私 （Confidentiality，Privacy)
- 完整性（Integrity）
  - 没有被修改或删除
- 可用性Availability (持久性，不可中断)
  - Denial of Service Attacks ； Virus that deletes files
- 不可否认性Non-repudiation
- 标准
  - ISO X.800：Security architecture for Open Systems Interconnection for CCITT application
  - IETF RFC 2828：Internet Security Glossary

安全机制

- 特点
  - feature designed to detect, prevent, or recover from a security attack
- 多种机制
  - 特定安全机制：特定协议层上执行
  - 普适安全机制：不指定特定OSI安全服务，跨层执行
  - no single mechanism that will support all services required
- 基础
  - 密码技术
    - 可逆密码编码机制
    - 不可逆密码编码机制

安全机制（X.800）

◆特定安全机制:
- ❖Encipherment加密, digital signatures数字签名
- ❖access controls访问控制
- ❖data integrity数据完整性
- ❖authentication exchange认证交换
- ❖traffic padding流量填充, routing control路由控制
- ❖notarization公证

◆普适安全机制:
- ❖trusted functionality可信功能
- ❖security labels安全标签
- ❖event detection事件检测
- ❖security audit trails安全审计跟踪
- ❖security recovery安全恢复

安全服务和机制的关系（表1.4）

Service	Mechanism							
	Enciph-erment	Digital signature	Access control	Data integrity	Authenti-cation exchange	Traffic padding	Routing control	Notari-zation
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

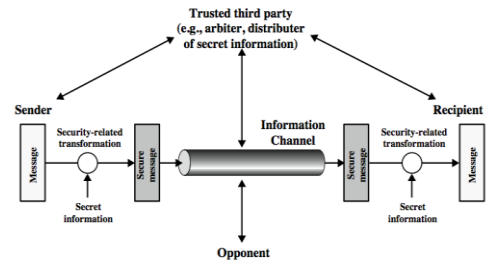
网络安全模型

◆网络加密安全模型

◆网络访问安全模型

网络加密安全模型

◆网络加密安全模型由三部分构成：参与者、信息通道和安全机制



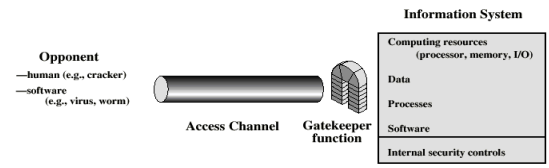
网络安全模型

◆ 设计安全服务的需求

1. 算法：design a suitable algorithm for the security transformation
2. 产生密钥：generate the secret information (keys) used by the algorithm
3. 分发密钥：develop methods to distribute and share the secret information
4. 安全协议：specify a protocol enabling the principals to use the transformation and secret information for a security service

网络访问安全模型

◆网络访问安全模型保护系统资源免受非授权的访问。模型由四部分构成：攻击者、访问信道、安全机制和资源系统。



相关标准化组织

- NIST（National Institute of Standards and Technology）
  - SHA
- Internet Engineering Task Force (IETF)
  - Internet标准：RFCxxxx
- ITU标准
  - X.509 Certificates
- IEEE
  - 802.3-Ethernet, 802.11 - Wireless LAN
- International Organization for Standardization (ISO)
- Department of Defense, Nat. Computer Security Center
  - Orange Book: Class A1, B3, C1, C2, ...
- 事实标准
  - De Facto (PGP email security system, Kerberos-MIT)

安全标准分类

- 类别
  - 密码标准
    - DES等
  - 协议标准
    - SSL等
  - 信息安全管理标准
    - ISO 17799等
  - 安全评估标准
    - TCSEC-ITSEC-CC等

研究资源

- 网络安全相关的国际会议
  - IEEE Symposium on Security and Privacy
  - ACM Conference on Computer and Communications Security
  - Usenix Security Symposium
  - ISOC Network and Distributed System Security Symposium
  - Annual Computer Security Applications Conference